

Amendments to the Drawings:

The attached sheet of drawings includes changes to Fig. 1. This sheet replaces the original sheet which included Fig. 1. In Fig. 1, previously omitted elements 12A and 18A have been added.

Attachment: Replacement Sheet
Annotated Sheet Showing Changes

Remarks

1. Introduction

Claims 1 and 7-29 are pending.

2. Drawings

The drawings were objected to as failing to show hard disk device 12A and hard disk device 18A. Applicants submit amended drawings to overcome the objection. No new matter is added by this amendment.

3. Oath/Declaration

The Office Action states that the title of the invention is missing from the declaration of the present application. Applicants have reviewed the declaration submitted, which indicates that the title "Communication Device and Program" is provided on the first sheet. Therefore, Applicants believe that the declaration submitted is acceptable.

4. Rejections under 35 U.S.C. § 101

Claims 1-6 were rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. Applicants cancel claim 6, rendering the rejection moot. Applicants further amend claim 1 where it is believed appropriate.

5. Claim objections

The Office Action objected to claims 1 and 6 as failing to clearly articulate the meaning of the recited limitations. Applicants amend claim 1 where it is believed appropriate, and cancel claim 6.

6. Rejections under 35 U.S.C. § 112, first paragraph

The Office Action rejected claims 1-6 under 35 U.S.C. § 112, first paragraph, stating that the application as filed does not provide any disclosure for the "receiving means" recited in Claims 1 and 6. In particular, the Office Action states that "the specification does not provide

disclosure what the receiving means consist of (e.g. antenna, a program routine, communicating unit, combination or all of the elements).

Applicants state that the present application provides examples of the receiving means. As merely one example, the specification discloses that communication unit 16F may comprise an antenna and a wireless communication unit, as discussed in paragraph [0043] of the present application (reproduced below):

Communicating unit 16F comprises an antenna and a wireless communication unit; wirelessly communicates data packets with mobile packet communication network 15, and relays data packets between CPU 16B and mobile packet communication network 15. Communicating unit 16F comprises a CODEC, a microphone and a speaker for voice communication; and enables mobile station 16 to conduct voice communication through a mobile telephone network (not shown) which has a line switching system.

Therefore, Applicants believe that the “receiving means” is adequately disclosed in the present application.

7. Rejections under 35 U.S.C. § 112, second paragraph

Claim 1 was rejected under 35 U.S.C. § 112, second paragraph based on a failure to disclose any structure for the “receiving means” in the present application. As stated above, the present application adequately discloses the “receiving means”.

8. Rejections under 35 U.S.C. §§ 102, 103

Claims 1-3 and 6 were rejected under 35 U.S.C. §102(b) as anticipated by or, in the alternative, under 35 U.S.C. § 103(a) as obvious over Schneier (Bruce Schneier, “Applied Cryptography, Protocols, Algorithms and Source Code in C,” 2nd edition, 1996 ISBN: 0471128457). Claims 1-6 were rejected under 35 U.S. C. § 103(a) as obvious over Rose (U.S. Patent No. 5,708,709) in view of Schneier (Bruce Schneier, “Applied Cryptography, Protocols, Algorithms and Source Code in C,” 2nd edition, 1996 ISBN: 0471128457).

The prior art (as discussed in the background of the present application and the cited Schneier reference) merely relied on two files in verifying a digital signature to determine whether application data should be executed: a first file containing the application data (sometimes termed a JAR file) and a second file (sometimes termed an Application Descriptor File). See paragraph [0007] of the present application. The Application Descriptor File includes

some description of the JAR file (such as a digital signature), and is used to verify the authenticity of the JAR file.

However, there is a serious deficiency in the prior art. Specifically, if the Application Descriptor File is unreliable, verifying the accuracy of the JAR file with the Application Descriptor File is unwise. To remedy this, the present application as claimed uses three files in the verification process. Specifically, data in the third file (termed “second file validity data”) is used to verify whether the second file is valid. See claims 1 and 18 (“generating a second file calculated value using the one-way function, at least a part of the second file being input to the one-way function to generate the second file calculated value”; “comparing the second file calculated value with the second file validity data in the third file”; and “determining whether the second file is valid based on the comparing of the second file calculated value with the second file validity data in the third file”). Further, data in the second file (termed “application validity data”) is used to verify whether the application data in the first file is valid. See claims 1 and 18 (“executing the application data on the communication device if the application data is verified using the application validity data in the second file”).

This use of three files in the verification process (such as a digital signature process) is significantly advantageous over the prior art. The verification results in the second file being more reliable (and therefore more usable when verifying the application data for execution in the first file). Moreover, the use of the third file separate from the first and second file provides additional advantages. The third file may be received from an entity separate from the first or second files (such as a trusted server), so that the verification of the second file may be more reliable. See claims 14 and 26.

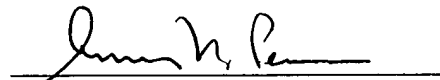
Further, the value that is analyzed in the second file (and used to compare with the third file) may be “independent data” (independent of the application data contained in the first file) (see claims 12 and 24), such as “certificate data for certifying authenticity of the application data, the certificate data being provided by a certificate authority.” See claims 13 and 25. In this way, even if the content of the application data changes, the contents of the third file does not need to be updated since the data in the second file used for verification is independent of the application data. For example, the digital signature of the certificate in the second file (which is stored in the third file) does not need to be updated even if the application data changes. This is in contrast to what may happen between the first and second file. Specifically, if the application data in the

first file is changed (such as updating an application program in the first file), the second file needs to be likewise updated to reflect the change (*e.g.*, the digital signature in the second file needs to be updated). In addition, the one-way function used to verify the second file may be the same one-way function used to verify the first file so that the same hash function may be used for the entire verification process. See claims 10 and 22. And, the second file may be verified before the first file is even received. See claims 16 and 28. Thus, the first file does not even need to be received before the second file is verified, reducing the possibility of downloading a first file that may cause problems on the communication device. For at least these reasons, the claims as currently presented distinguish over the cited art.

9. Conclusion

The Examiner is invited to contact the undersigned attorneys for the Applicant via telephone if such communication would expedite this application.

Respectfully submitted,



Amir N. Penn
Registration No. 40,767
Attorney for Applicant

BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, ILLINOIS 60610
(312) 321-4200

1/5

FIG. 1

